UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/581,445 | 06/02/2006 | Masao Nonaka | 2006_0778A | 6614 |

52349 7590 01/27/2010

WENDEROTH, LIND & PONACK L.L.P.
1030 15th Street, N.W.
Suite 400 East
Washington, DC 20005-1503

| EXAMINER | |
|---|---|
| YANG, JAMES J | |
| ART UNIT | PAPER NUMBER |
| 2612 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 01/27/2010 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/581,445 | NONAKA ET AL. | |
| | Examiner | Art Unit | |
| | JAMES YANG | 2612 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *02 June 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 June 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *06/02/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

### *Specification*

The disclosure is objected to because of the following informalities:

Page 2, Line 7, the phrase "identification information is has prestored" should be changed to something similar to –identification information that has been prestored--.

Page 50, Line 3, the phrase "on example of which" should be changed to –one example of which--.

Page 50, Line 17, "the visitor" should be removed.

Appropriate correction is required.

### *Claim Rejections - 35 USC § 101*

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 47 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 47 claims "An authentication program…". The program claimed per se is not claimed as embodied/encoded in computer-readable media and is thus non-statutory, i.e. "When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the

descriptive material to be realized". A program by itself is not a computer, nor machine, nor manufacture, nor composition of matter, and is therefore non-statutory.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claim 1-7, 12, 16, 31-34, 36-37, 39-41, 43-44, and 46-48 are rejected under 35 U.S.C. 102(e) as being anticipated by Ahlstrom et al. (U.S. 2003/0081747).

Claims 1, 31, 46-48 Ahlstrom teaches:

**An authentication system, apparatus, method, program, and computer-readable program recording medium (**Ahlstrom, Paragraph [0003]**), comprising:**

**a portable recording medium which a forwarding agent has (**Ahlstrom, Paragraph [0031], A card read by a card reader is a portable recording medium, and the user is a forwarding agent.**);**

**an authentication apparatus operable to verify authenticity of a visit by the forwarding agent (**Ahlstrom, Fig. 1: 116, Paragraph [0031], The system selectively grants access based on the access code read from the card.**), the authentication**

**apparatus being provided in a residence (**Ahlstrom, Fig. 1: 112, 114, Paragraph [0022], As can be seen from Figure 1, the card readers 112 and 114 are located adjacent to the gate 108 of the building. The system can be implemented in a place of residence (see Ahlstrom, Paragraph [0026]).**) of a person who is visited by the forwarding agent (**Ahlstrom, Paragraph [0026], Ahlstrom further discloses issuing temporary access cards, which is here interpreted as cards for people who only temporarily need access to the entrance by way of cards (see Paragraph [0035]). Therefore, these people may be interpreted as visitors.**); and**

**an input/output apparatus operable to perform inputting and outputting of information between the portable recording medium and the authentication apparatus (**Ahlstrom, Paragraph [0022], The system has two card readers, one inside and one outside the building. The card readers are in communication with the main unit.**), the input/output apparatus being provided at an entrance of the residence (**Ahlstrom, Fig. 1: 112, 114, Paragraph [0022], As can be seen from Figure 1, the card readers 112 and 114 are located adjacent to the gate 108 of the building.**),**

**wherein the portable recording medium stores therein in advance at least one piece of information concerning authenticity of the visit by the forwarding agent (**Ahlstrom, Paragraph [0031], The cards have access codes on them, which is used to determine accessibility.**), and**

**the authentication apparatus and an information storage unit stores therein at least one piece of information used for verifying authenticity of the visit by the forwarding agent (**Ahlstrom, Paragraph [0028]**), and a judgment unit that judges**

**whether or not the visit by the forwarding agent is authentic by, via the input/output apparatus, performing an authentication using the information stored in the portable recording medium and the information stored in the authentication apparatus and information storage unit (**Ahlstrom, Paragraph [0031]**).**

Claims 2 and 32, Ahlstrom further teaches:

**The portable recording medium is an IC card (**Ahlstrom, Paragraph [0032], It is known in the art that a smart card is a type of IC (Integrated Circuit) card.**),**

**the input/output apparatus is a card reader for the IC card (**Ahlstrom, Paragraph [0032], It is well-known in the art that a card reader capable of reading a smart card is a card reader for an IC card.**),**

**the card reader detects a lock status of an entrance door (**Ahlstrom, Paragraphs [0022] and [0030], The system has sensors to detect whether a door is opened or close. It is well-known in the art that doors in a controlled access system are locked when the door is closed, thus the sensors are capable of determining the lock status of the door.**), and**

**the authentication apparatus and judgment unit performs the authentication if the card reader detects that the entrance door is locked (**Ahlstrom, Paragraph [0045], It is well-known in the art that TES systems lock a door or gate when the door or gate is closed. Thus, the system requires a user to enter a code or scan a card when entrance is requested. If the door or gate is in the open state

without authorization, then an alarm is sounded. Thus, the system performs the authentication process when the door is locked and the alarm is not sounded.).

Claims 3 and 33, Ahlstrom further teaches:

**The IC card stores therein certification information that certifies authenticity of the forwarding agent, as the information concerning authenticity of the visit by the forwarding agent (**Ahlstrom, Paragraph [0031], The cards have access codes on them, which is used to determine accessibility. The access codes are thus certification information stored on the IC card that is used to certify authenticity.**),**

**the authentication apparatus and information storage unit stores therein, as the information concerning verifying authenticity of the visit by the forwarding agent, authentication information that is used to examine the certification information (**Ahlstrom, Fig. 1: 116, Paragraph [0031], The system selectively grants access based on the access code read from the card. The authentication apparatus has a list of authorized access codes (see Paragraph [0028]).**), and**

**the authentication apparatus and judgment unit performs, via the card reader, the authentication using the certification information and the stored authentication information to judge whether or not the visit by the forwarding agent is authentic (**Ahlstrom, Paragraph [0031]**).**

Claims 4 and 34, Ahlstrom teaches:

**The IC card stores first visit information that indicates a business of the visit by the forwarding agent, as the information concerning authenticity of the visit by the forwarding agent (**Ahlstrom, Paragraph [0035], The IC cards store access codes (see Paragraph [0031]) which are used by the system to determine authenticity of the card holder. Because the access codes of the cards may also be used to determine whether a specific card and thus the cardholder is under a time restriction, the access codes on the IC card may generally be interpreted as including first visit information embedded in it to indicate to the system that the person holding the IC card has a limited time period of accessibility. Thus, the access code indicates that the user of the card wants entry and for a specified period of time.**),**

**the authentication apparatus further stores therein, as the information concerning verifying authenticity of the visit by the forwarding agent, second visit information used to examine the first visit information (**Ahlstrom, Paragraph [0035], The system is programmed to recognize an access code as having time restrictions, thus the access code also serves as information concerning authenticity. The time restrictions are thus second visit information, and the access codes are stored in the main unit (see Paragraph [0028]).**),**

**the authentication apparatus and judgment unit, if a result of the authentication using the certification information and the authentication information is positive, acquires the first visit information from the IC card via the card reader, judges whether or not the acquired first visit information matches the stored second visit information, and if a result of the judgment is positive,**

**judges that the visit by the forwarding agent is authentic (**Ahlstrom, Paragraph [0035], The card reader retrieves the code from the card (see Paragraph [0031]), the system then determines if the code is valid, and then the system further determines from the retrieved code whether the card corresponds to a specific time restriction.**).**

Claim 5, Ahlstrom further teaches:

**The first visit information is first time information that indicates a time period for the visit by the forwarding agent (**Ahlstrom, Paragraph [0035]**),**

**the second visit information is second time information that indicates a time period for the visit by the forwarding agent (**Ahlstrom, Paragraph [0035], The system is programmed to know, based on the access code, whether or not the card has a time restriction on it.**), and**

**the authentication apparatus judges whether or not the first time information matches the second time information (**Ahlstrom, Paragraph [0035], Also in Paragraph [0031] the system determines if the access code retrieved from the IC card matches the access codes stored in the main unit.**).**

Claim 6, Ahlstrom further teaches:

**The first visit information is first business information that indicates a business of the visit by the forwarding agent (**Ahlstrom, Paragraph [0035], Temporary cards are programmed to only work for a certain time period, or for a certain number of times. Thus, the time periods and times are also considered as the business

of the visit, because it signifies to the system that the user wants entry to the area in a specified time period The term "business" is here interpreted as meaning "purpose".**),**

**the second visit information is second business information that indicates a business of the visit by the forwarding agent (**Ahlstrom, Fig. 1: 116, Paragraph [0031], The system selectively grants access based on the access code read from the card. The authentication apparatus has a list of authorized access codes (see Paragraph [0028]).**), and**

**the authentication apparatus judges whether or not the first business information matches the second business information (**Ahlstrom, Paragraph [0035], The card reader retrieves the code from the card (see Paragraph [0031]), the system then determines if the code is valid, and then the system further determines from the retrieved code whether the card corresponds to a specific time restriction.**).**

Claim 7, Ahlstrom further teaches:

**The first visit information includes (i) first time information that indicates a time period for the visit by the forwarding agent and (ii) first business information that indicates a business of the visit by the forwarding agent (**Ahlstrom, Paragraph [0035], Because the system can recognize, based on the access code, when the user wishes to gain access to the door, the access code itself, which is first visit information, includes information embedded in it that indicates a time period and also business information.**),**

**the second visit information includes (iii) second time information that indicates a time period for the visit by the forwarding agent and (iv) second business information that indicates a business of the visit by the forwarding agent (**Ahlstrom, Paragraphs [0031] and [0035], Because a list of access codes are stored at the authentication apparatus and the access codes are interpreted as first visit information, the list represents a list of second visit information that are the same values as the first visit information, which includes time information and business.**), and**

**the authentication apparatus judges whether or not the first time information matches the second time information, and judges whether or not the first business information matches the second business information (**Ahlstrom, Paragraphs [0031] and [0035]**).**

Claim 12, 36, and 43, Ahlstrom further teaches:

**The IC card further stores therein visitor information for identifying a visitor (**Ahlstrom, Paragraph [0031], The cards have access codes on them, which is used to determine accessibility. Thus the IC card has a visitor information storage unit**),**

**the authentication apparatus further acquires the visitor information from the IC card via the card reader (**Ahlstrom, Paragraph [0022], The system has two card readers, one inside and one outside the building. The card readers are in communication with the main unit. The authentication apparatus includes a visitor information acquiring unit, and the IC card has an output unit.**), and if the authentication apparatus judges that the visit by the forwarding agent is**

**authentic, displays the visitor information on a visitor information display unit** (Ahlstrom, Paragraph [0036])**.**

Claim 16, 37, and 44, Ahlstrom further teaches:

**The authentication apparatus and the IC card perform a challenge-response authentication process using the certification information and the authentication information (**Ahlstrom, Paragraphs [0031], The system retrieves the access code stored on the card and determines if the access code matches a code stored in the database. The matching of codes is hereby interpreted as a challenge-response authentication process. Furthermore, the authentication information is the access code stored in authentication apparatus (see Ahlstrom, Paragraph [0028]), and the certification is the access code stored in the IC card.**).**

Claim 39, Ahlstrom teaches:

**A portable recording medium which a forwarding agent has (**Ahlstrom, Paragraph [0031], A card read by a card reader is a portable recording medium, and the user is a forwarding agent.**) and is used by an authentication apparatus operable to verify authenticity of a visit by the forwarding agent (**Ahlstrom, Fig. 1: 116, Paragraph [0031], The system selectively grants access based on the access code read from the card.**), the authentication apparatus being provided in a residence** (Ahlstrom, Fig. 1: 112, 114, Paragraph [0022], As can be seen from Figure 1, the card readers 112 and 114 are located adjacent to the gate 108 of the building. The system

can be implemented in a place of residence (see Ahlstrom, Paragraph [0026]).**) of a person who is visited by the forwarding agent (**Ahlstrom, Paragraph [0026], Ahlstrom further discloses issuing temporary access cards, which is here interpreted as cards for people who only temporarily need access to the entrance by way of cards (see Paragraph [0035]). Therefore, these people may be interpreted as visitors.**), the portable recording medium comprising:**

**a storage unit operable to store therein in advance at least one piece of information concerning authenticity of the visit by the forwarding agent (**Ahlstrom, Paragraph [0031], The cards have access codes on them, which is used to determine accessibility.**);**

**a receiving unit operable to receive first data from the authentication apparatus (**Ahstrom, Paragraph [0031], The system verifies the access code stored on the portable medium. Thus, the card reader interrogation signal, as is known in the art, to the smart card is a first data from the input/output apparatus.**) via an input/output apparatus provided at an entrance of the residence (**Ahlstrom, Fig. 1: 112, 114, Paragraph [0022], As can be seen from Figure 1, the card readers 112 and 114 are located adjacent to the gate 108 of the building.**);**

**a data generating unit operable to generate second data from the first data using the information stored in the storage unit, the second data being used for an authentication process (**Ahstrom, Paragraph [0031], The portable recording medium returns data stored on the smart card to the authentication apparatus in

response to the interrogation signal of the card reader. The response is thus second data.**); and**

**an output unit operable to output the second data to the authentication apparatus via the input/output apparatus (**Ahstrom, Paragraph [0031], It is well—known in the art that smart cards are able to respond to interrogation signals by using an input/output device, depending upon the type of smart card used.**).**

Claim 40, Ahlstrom further teaches:

**The storage unit stores therein certification information that certifies authenticity of the forwarding agent, as the information concerning authenticity of the visit by the forwarding agent (**Ahlstrom, Paragraph [0031], The cards have access codes on them, which is used to determine accessibility. The access codes are thus certification information stored on the IC card that is used to certify authenticity.**), and the data generating unit generates the second data using the certification information (**Ahlstrom, Paragraph [0031], The data generating unit of the smart card sends its access code to the authentication apparatus for authentication.**).**

Claim 41, Ahlstrom further teaches:

**The storage unit further stores therein visit information that indicates a business of the visit by the forwarding agent, as the information concerning authenticity of the visit by the forwarding agent (**Ahlstrom, Paragraph [0035], The IC cards store access codes (see Paragraph [0031]) which are used by the system to

determine authenticity of the card holder. Because the access codes of the cards may also be used to determine whether a specific card and thus the cardholder is under a time restriction, the access codes on the IC card may generally be interpreted as including first visit information embedded in it to indicate to the system that the person holding the IC card has a limited time period of accessibility. Thus, the access code indicates that the user of the card wants entry and for a specified period of time.**), and the output unit further outputs the visit information to the authentication apparatus via the input/output apparatus (**Ahlstrom, Paragraph [0035], The card reader retrieves the code from the card (see Paragraph [0031]), the system then determines if the code is valid, and then the system further determines from the retrieved code whether the card corresponds to a specific time restriction.**).**

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 8-11, 35, and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ahlstrom et al. (U.S. 2003/0081747) in view of Hill et al. (U.S. 6431453).

Claims 8, 35, and 42, Ahlstrom teaches:

**The IC card stores information identifying the forwarding agent (**Ahlstrom, Paragraph [0031], The cards have access codes on them, which is used to determine accessibility.**) and displays information read from the IC card (**Ahlstrom, Paragraph [0036]**).**

Ahlstrom does not teach:

**The IC card further stores therein article information concerning an article delivered by the forwarding agent, and**

**the authentication apparatus and an article information acquiring unit further acquires the article information from the IC card via the card reader, and if the authentication apparatus judges that the visit by the forwarding agent is authentic, displays the article information using an article information display unit.**

Hill teaches:

**The IC card further stores therein article information concerning an article delivered by the forwarding agent (**Hill, Col. 3, Lines 30-35, Where the information stored on the IC chip 32 is account information, as is known in the prior art (see Hill, Col. 1, Lines 39-44). The IC card thus has an article information storage unit**), and**

**the authentication apparatus and further acquires the article information from the IC card via the card reader, and authenticates the article information (**Hill,

Col. 4, Lines 20-27, The authentication apparatus has an article information acquiring unit, and also an output unit.**).**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the smart card in Ahlstrom by integrating the teaching of storing information about a carrier as taught by Hill to be displayed on a display.

The motivation would be to increase the overall security to residents of the system by providing a way to verify packages being delivered by using known data storage capabilities of IC cards (see Hill, Col. 1, Lines 28-44). One of ordinary skill will recognize that allowing the system to verify information, such as the recipient of the package, would help identify the package prior to opening.

Claim 9, Ahlstrom in view of Hill further teaches:

**The article information is a name of a sender of the article (**Hill, Col. 1, Lines 28-44, It would have been obvious to one of ordinary skill in the art that the name of the sender, such as the vendor of a product, would be considered account information.**), and**

**the authentication apparatus acquires the name of the sender from the IC card (**Hill, Col. 4, Lines 20-27**) and displays the acquired name (**Ahlstrom, Paragraph [0036]**).**

Claim 10, Ahlstrom in view of Hill further teaches:

**The article information is a name of the article (**Hill, Col. 1, Lines 28-44, It would have been obvious to one of ordinary skill in the art that the name of the article, such as the name of a product, would be considered account information.**), and**

**the authentication apparatus acquires the name of the article from the IC card (**Hill, Col. 4, Lines 20-27**) and displays the acquired name of the article (**Ahlstrom, Paragraph [0036]**).**

Claim 11, Ahlstrom in view of Hill further teaches:

**The article information is a message from a sender of the article (**Hill, Col. 1, Lines 28-44, It would have been obvious to one of ordinary skill in the art that a message from a sender of the article, such as advertising or product information from a vendor, would be considered account information.**), and**

**the authentication apparatus acquires the message from the IC card (**Hill, Col. 4, Lines 20-27**) and displays the acquired message (**Ahlstrom, Paragraph [0036]**).**

3. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ahlstrom et al. (U.S. 2003/0081747) in view of Kinugasa et al. (U.S. 5898165).

Claim 13, Ahlstrom does not teach:

**The visitor information is a name of the visitor, and**

**the authentication apparatus acquires the name of the visitor from the IC card and displays the acquired name of the visitor.**

Kinugasa teaches:

**Storing the name of a person on an IC card (**Kinugasa, Col. 4, Lines 33-35**), and**

**the authentication apparatus acquires the name of the visitor from the IC card and displays the acquired name of the visitor (**Kinugasa, Col. 4, Lines 27-35**).**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the smart card in Ahlstrom by incorporating the teaching of storing the name of a person into an IC card as taught by Kinugasa.

The motivation would be to provide addition information to further verify the identity of the person wanting access to the building. One of ordinary skill in the art would recognize that having more data fields for verification would improve the ability of the system to identify a person, thus improving the overall security of the system.

4. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ahlstrom et al. (U.S. 2003/0081747) in view of Yasuda et al. (U.S. 4703347).

Claim 14, Ahlstrom does not teach:

**The visitor information is an image of a facial photo of the visitor, and**

**the authentication apparatus acquires the image of the facial photo of the visitor from the IC card and displays the acquired image of the facial photo.**

Yasuda teaches:

**Storing an image of a facial photo of a person in an IC card (**Yasuda, Col. 3, Lines 23-29**), and**

**an authentication apparatus acquires the image of the facial photo of the visitor from the IC card and displays the acquired image of the facial photo (**Yasuda, Col. 3, Lines 35-42**).**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the smart card in Ahlstrom by incorporating the teaching of storing a photo of a person into an IC card as taught by Yasuda.

The motivation would be to provide a more reliable way to identify a person using individuality discriminating information (see Yasuda, Col. 2, Lines 20-30).

5. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ahlstrom et al. (U.S. 2003/0081747) in view of Kinugasa et al. (U.S. 5898165), and further in view of Yasuda et al. (U.S. 4703347).

Claim 15, Ahlstrom does not teach:

**The visitor information is a name and an image of a facial photo of the visitor, and**

**the authentication apparatus acquires the name and the image of the facial photo of the visitor from the IC card and displays the acquired name and image of the facial photo.**

Kinugasa teaches:

**Storing the name of a person on an IC card (**Kinugasa, Col. 4, Lines 33-35**), and**

**the authentication apparatus acquires the name of the visitor from the IC card and displays the acquired name of the visitor (**Kinugasa, Col. 4, Lines 27-35**).**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the smart card in Ahlstrom by incorporating the teaching of storing the name of a person into an IC card as taught by Kinugasa.

The motivation would be to provide addition information to further verify the identity of the person wanting access to the building. One of ordinary skill in the art would recognize that having more data fields for verification would improve the ability of the system to identify a person, thus improving the overall security of the system.

Ahlstrom in view of Kinugasa does not teach:

**The visitor information is a facial photo, and the authentication apparatus acquires the image of the facial photo.**

Yasuda teaches:

**Storing an image of a facial photo of a person in an IC card (**Yasuda, Col. 3, Lines 23-29**), and**

**an authentication apparatus acquires the image of the facial photo of the visitor from the IC card and displays the acquired image of the facial photo (**Yasuda, Col. 3, Lines 35-42**).**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the smart card in Ahlstrom in view of Kinugasa by incorporating the teaching of storing a photo of a person into an IC card as taught by Yasuda.

The motivation would be to provide a more reliable way to identify a person using individuality discriminating information (see Yasuda, Col. 2, Lines 20-30).

6. Claims 17, 20-21, and 26-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ahlstrom et al. (U.S. 2003/0081747) in view of Abraham et al. (U.S. 4799061).

Claim 17, Ahlstrom teaches:

**The authentication generates challenge data, and outputs the generated challenge data to the IC card via the card reader, the IC card receives the challenge data from the authentication apparatus, and the authentication apparatus receives the response data from the IC card (**Ahlstrom, Paragraphs [0022] and [0031], The system has two card readers, one inside and one outside the building. The card readers are in communication with the main unit. The term challenge data is interpreted as the interrogation signal as is well known in the art.**), and judges whether or not the access code received from the smart card matches the access code stored in memory (**Ahlstrom, Paragraphs [0028] and [0031]**).**

Ahlstrom does not teach:

**The certification information is an encryption key,**

**the authentication information is a decryption key,**

**the authentication apparatus generates challenge data, and outputs the generated challenge data to the IC card via the card reader,**

**the IC card receives the challenge data from the authentication apparatus, generates response data by encrypting by encrypting the challenge data using the encryption key, and outputs the generated response data to the authentication apparatus via the card reader, and**

**the authentication apparatus receives the response data from the IC card, generates decrypted data by decrypting the response data using the decryption**

**key, and performs an authentication by judging whether or not the generated decrypted data matches the challenge data.**

Abraham teaches:

**The certification information is an encryption key (**Abraham, Col. 3, Lines 5-8, The certification information is the secret keyed stored on the card.**),**

**the authentication information is a decryption key (**Abraham, Col. 3, Lines 5-8, The authentication information is the secret key stored in the terminal.**),**

**the authentication apparatus generates challenge data, and outputs the generated challenge data to the IC card via the card reader (**Abraham, Col. 3, Lines 13-21, Terminal 20 transmits and receives information to and from the card, respectively, and thus is interpreted as a card reader.**),**

**the IC card receives the challenge data from the authentication apparatus, generates response data by encrypting the challenge data using the encryption key, and outputs the generated response data to the authentication apparatus via the (**Abraham, Col. 3, Lines 25-28**), and**

**the authentication apparatus receives the response data from the IC card, generates decrypted data by decrypting the response data using the decryption key (**Abraham, Col. 3, Lines 28-30**), and performs an authentication by judging whether or not the generated decrypted data matches the challenge data (**Abraham, Col. 3, Lines 30-34**).**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the access control system in Ahlstrom by incorporating the teaching of a challenge response authentication system as taught by Abraham.

The motivation would be to protect useful information by first authenticating all components in an authentication system (see Abraham, Col. 1, Lines 63-66).

Claim 20, Ahlstrom teaches:

**The authentication generates challenge data, and outputs the generated challenge data to the IC card via the card reader, the IC card receives the challenge data from the authentication apparatus, and the authentication apparatus receives the response data from the IC card** (Ahlstrom, Paragraphs [0022] and [0031], The system has two card readers, one inside and one outside the building. The card readers are in communication with the main unit. The term challenge data is interpreted as the interrogation signal as is well known in the art.)**, and judges whether or not the access code received from the smart card matches the access code stored in memory** (Ahlstrom, Paragraphs [0028] and [0031])**, and**

**a card reader** (Ahlstrom, Fig. 1: 112, 114)**.**

Ahlstrom does not teach:

**The authentication information is a secret key,**

**the IC card stores therein a first key that is obtained by executing a one-way function on a key that is identical with the secret key,**

**the authentication apparatus generates challenge data, and outputs the generated challenge data to the IC card via the card reader,**

**the IC card receives the challenge data from the authentication apparatus, generates response data by encrypting the challenge data using the first key, and outputs the generated response data to the authentication apparatus via the card reader, and**

**the authentication apparatus receives the response data from the IC card, generates a second key by executing a function, which is identical with the one-way function, on the secret key, generates decrypted data by decrypting the response data using the second key, and performs an authentication by judging whether or not the generated decrypted data matches the challenge data.**

Abraham teaches:

**The authentication information is a secret key (**Abraham, Col. 3, Lines 4-8**),**

**the IC card stores therein a first key that is obtained by executing a one-way function on a key that is identical with the secret key (**Abraham, Col. 3, Lines 4-8, The one-way function is the decryption process of a value to obtain a random number RN (see Abraham, Col. 3, Lines 23-25)**.),**

**the authentication apparatus generates challenge data, and outputs the generated challenge data to the IC card via the card reader (**Abraham, Col. 3, Lines 13-21, Terminal 20 transmits and receives information to and from the card, respectively, and thus is interpreted as a card reader.**),**

**the IC card receives the challenge data from the authentication apparatus, generates response data by encrypting the challenge data using the first key, and outputs the generated response data to the authentication apparatus via the card reader (**Abraham, Col. 3, Lines 25-28**), and**

**the authentication apparatus receives the response data from the IC card, generates a second key by executing a function, which is identical with the one-way function, on the secret key (**Abraham, Col. 3, Lines 28-30, Where the terminal 20 decrypts the value Z with the secret key in order to obtain a value A. Since the secret keys are the same, the one-way functions are also the same.**), generates decrypted data by decrypting the response data using the second key (**Abraham, Col. 3, Lines 28-30**), and performs an authentication by judging whether or not the generated decrypted data matches the challenge data (**Abraham, Col. 3, Lines 30-34**).**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the access control system in Ahlstrom by incorporating the teaching of a challenge response authentication system as taught by Abraham.

The motivation would be to protect useful information by first authenticating all components in an authentication system (see Abraham, Col. 1, Lines 63-66).

Claim 21, Ahlstrom teaches:

**The authentication generates challenge data, and outputs the generated challenge data to the IC card via the card reader, the IC card receives the**

**challenge data from the authentication apparatus, and the authentication apparatus receives the response data from the IC card (**Ahlstrom, Paragraphs [0022] and [0031], The system has two card readers, one inside and one outside the building. The card readers are in communication with the main unit. The term challenge data is interpreted as the interrogation signal as is well known in the art.**), and judges whether or not the access code received from the smart card matches the access code stored in memory (**Ahlstrom, Paragraphs [0028] and [0031]**), and**

**a card reader (**Ahlstrom, Fig. 1: 112, 114**).**

Ahlstrom does not teach:

**The authentication information is a first secret key,**

**the IC card stores therein a second secret key that is identical with the first secret key, the authentication apparatus generates challenge data, and outputs the generated challenge data to the IC card via the card reader,**

**the IC card receives the challenge data from the authentication apparatus, generates response data by encrypting the challenge data using the second secret key, and outputs the generated response data to the authentication apparatus via the card reader, and**

**the authentication apparatus receives the response data from the IC card, generates encrypted data by encrypting the challenge data using the first secret key, and performs an authentication by judging whether or not the generated encrypted data matches the response data.**

Abraham teaches:

**The authentication information is a first secret key (**Abraham, Col. 3, Lines 4-8**),**

**the IC card stores therein a second secret key that is identical with the first secret key (**Abraham, Col. 3, Lines 4-8**), the authentication apparatus generates challenge data, and outputs the generated challenge data to the IC card via the card reader (**Abraham, Col. 3, Lines 13-21, Terminal 20 transmits and receives information to and from the card, respectively, and thus is interpreted as a card reader.**),**

**the IC card receives the challenge data from the authentication apparatus, generates response data by encrypting the challenge data using the second secret key, and outputs the generated response data to the authentication apparatus via the card reader (**Abraham, Col. 3, Lines 25-28**), and**

**the authentication apparatus receives the response data from the IC card, generates decrypted data by decrypting the challenge data using the first secret key (**Abraham, Col. 3, Lines 28-30**), and performs an authentication by judging whether or not the generated decrypted data matches the response data (**Abraham, Col. 3, Lines 30-34**).**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the access control system in Ahlstrom by incorporating the teaching of a challenge response authentication system as taught by Abraham.

The motivation would be to protect useful information by first authenticating all components in an authentication system (see Abraham, Col. 1, Lines 63-66).

As per the limitation of the authentication apparatus generates **encrypted** data by **encrypting** the challenge data using the first secret key, and performs an authentication by judging whether or not the generated **encrypted** data matches the response data, it would have been obvious to one of ordinary skill in the art to modify the authentication system in Abraham by comparing the encrypted data instead of the decrypted data, since both the terminal and the card encrypt data using the same secret key (see Abraham, Col. 3, Lines 4-8). Thus, a comparison of whether value X transmitted to the card is the same as value Z transmitted by the card could be made to determine whether the data matches.

Claim 26, Ahlstrom teaches:

**The authentication generates challenge data, and outputs the generated challenge data to the IC card via the card reader, the IC card receives the challenge data from the authentication apparatus, and the authentication apparatus receives the response data from the IC card (**Ahlstrom, Paragraphs [0022] and [0031], The system has two card readers, one inside and one outside the building. The card readers are in communication with the main unit. The term challenge data is interpreted as the interrogation signal as is well known in the art.**), and**

**judges whether or not the access code received from the smart card matches the access code stored in memory (**Ahlstrom, Paragraphs [0028] and [0031]**), and**

**a card reader (**Ahlstrom, Fig. 1: 112, 114**).**

Ahlstrom does not teach:

**The IC card stores therein a second visit key that is identical with a first visit key that is distributed from the forwarding agent to the authentication apparatus prior to the visit,**

**the authentication apparatus further stores therein the first visit key,**

**if a result of an authentication by a challenge-response is positive, the authentication apparatus further generates visit examination data, and outputs the generated visit examination data to the IC card via the card reader,**

**the IC card receives the visit examination data from the authentication apparatus, generates encrypted visit examination data by encrypting the received visit examination data using the second visit key, and outputs the generated encrypted visit examination data to the authentication apparatus via the card reader, and**

**the authentication apparatus receives the encrypted visit examination data from the IC card, decrypts the encrypted visit examination data using the first visit key, judges whether or not a result of the decrypting matches the visit examination data, and if it judges that the result of the decrypting matches the**

**visit examination data, judges whether or not first visit information matches second visit information.**

Abraham teaches:

**The IC card stores therein a second visit key that is identical with a first visit key that is distributed from the forwarding agent to the authentication apparatus prior to the visit (**Abraham, Col. 3, Lines 4-8, The secret keys are stored in the smart cards and the terminal beforehand.**),**

**the authentication apparatus further stores therein the first visit key (**Abraham, Col. 3, Lines 4-8**),**

**if a result of an authentication by a challenge-response is positive (**Abraham, Col. 2, Lines 65-68 through Col. 3, Lines 1-3, The terminal 20 must first detect the presence of a smart card before authenticating it, so the detection as is known in the art, is hereby interpreted as a challenge-response.**), the authentication apparatus further generates visit examination data, and outputs the generated visit examination data to the IC card via the card reader (**Abraham, Col. 3, Lines 13-21, Terminal 20 transmits and receives information to and from the card, respectively, and thus is interpreted as a card reader. Also, visit examination data is generally interpreted as attempting to identify the IC card during the authentication process.**),**

**the IC card receives the visit examination data from the authentication apparatus, generates encrypted visit examination data by encrypting the received visit examination data using the second visit key, and outputs the generated**

**encrypted visit examination data to the authentication apparatus via the card reader (**Abraham, Col. 3, Lines 25-28**), and**

**the authentication apparatus receives the encrypted visit examination data from the IC card, decrypts the encrypted visit examination data using the first visit key (**Abraham, Col. 3, Lines 28-30**), judges whether or not a result of the decrypting matches the visit examination data, and if it judges that the result of the decrypting matches the visit examination data, judges whether or not first visit information matches second visit information (**Abraham, Col. 3, Lines 30-34**).**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the access control system in Ahlstrom by incorporating the teaching of a challenge response authentication system as taught by Abraham.

The motivation would be to protect useful information by first authenticating all components in an authentication system (see Abraham, Col. 1, Lines 63-66).

Claim 27, Ahlstrom does not teach:

**When the authentication apparatus outputs the challenge data to the IC card, the authentication apparatus converts the challenge data into converted challenge information that has the same contents as the challenge data but has a different data structure from the challenge data, and outputs, to the IC card, the converted challenge information as the challenge data.**

Abraham teaches:

**When the authentication apparatus outputs the challenge data to the IC card, the authentication apparatus converts the challenge data into converted challenge information that has the same contents as the challenge data but has a different data structure from the challenge data (**Abraham, Col. 3, Lines 25-28, The challenge data is the random number generated, and it is well-known the in art that the encryption process changes the data structure.**), and outputs, to the IC card, the converted challenge information as the challenge data (**Abraham, Col. 3, Lines 25-28**).**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the access control system in Ahlstrom by incorporating the teaching of a challenge response authentication system as taught by Abraham.

The motivation would be to protect useful information by first authenticating all components in an authentication system (see Abraham, Col. 1, Lines 63-66).

Claim 28, Ahlstrom in view of Abraham further teaches:

**When the IC card outputs the response data to the authentication apparatus, the IC card converts the response data into converted response information that has the same contents as the response data but has a different data structure from the response data (**Abraham, Col. 3, Lines 25-28, It is well-known in the art that encrypting data changes the data structure.**), and outputs, to the**

**authentication apparatus, the converted response information as the response data (**Abraham, Col. 3, Lines 25-28**).**

7. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ahlstrom et al. (U.S. 2003/0081747) in view of Abraham et al. (U.S. 4799061), and further in view of Yasukura (U.S. 6990588).

Claim 18, Ahlstrom in view of Abraham does not teach:

**The encryption key is holder certification information that shows biometric characteristics of a holder of the IC card, and**

**the authentication apparatus further receives holder authentication information that shows biometric characteristics of a visitor, and uses the holder authentication information as the decryption key.**

Yasukura teaches:

**The encryption key is holder certification information that shows biometric characteristics of a holder of the IC card (**Yasukura, Col. 19, Lines 9-11, The IC card has memory installed that stores biological individuality data. The data is also encrypted (see Yasukura, Col. 17, Lines 43-47).**), and**

**the authentication apparatus further receives holder authentication information that shows biometric characteristics of a visitor, and uses the holder authentication information as the decryption key (**Yasukura, Col. 17, Lines 43-50,

The authentication card read/write control part 411 receives the information from the IC card, and decodes the information.**).**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the smart card with encryption keys in Ahlstrom in view of Abraham, by integrating the teaching of encrypted biological individuality data as taught by Yasukura.

The motivation would be to provide additional information for identifying a person while maintaining secured information using known cryptography techniques (see Yasukura, Col. 4, Lines 35-45).

8. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ahlstrom et al. (U.S. 2003/0081747) in view of Abraham et al. (U.S. 4799061), and further in view of Lewis (U.S. 5761306).

Claim 19, Ahlstrom in view of Abraham does not teach:

**The authentication apparatus is connected, via a network, to a distribution apparatus that distributes the decryption key,**

**the authentication apparatus receives the decryption key distributed from the distribution apparatus and stores the received decryption key prior to the visit by the forwarding agent.**

Lewis teaches:

**The authentication apparatus is connected, via a network, to a distribution apparatus that distributes the decryption key (**Lewis, Col. 7, Lines 20-22**),**

**the authentication apparatus receives the decryption key distributed from the distribution apparatus and stores the received decryption key prior to the visit by the forwarding agent (**Lewis, Col. 7, Lines 29-34**).**

Therefore, it would have been obvious to one of ordinary skill in the art to modify the authentication system in Ahlstrom in view of Abraham by incorporating the teaching of sending new keys over a secure channel as taught by Lewis.

The motivation would be to update the keys of the system in case the keys are stolen (see Lewis, Col. 7, Lines 18-25). Furthermore, it would be obvious to one of ordinary skill in the art that the system would also be capable of adding new keys to the key server when new users (or nodes) are added to the system (see Lewis, Col. 6, Lines 24-35).

9. Claims 22 and 24-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ahlstrom et al. (U.S. 2003/0081747) in view of Gasser et al. (U.S. 5224163).

Claim 22, Ahlstrom teaches:

**The authentication generates challenge data, and outputs the generated challenge data to the IC card via the card reader, the IC card receives the**

**challenge data from the authentication apparatus, and the authentication apparatus receives the response data from the IC card (**Ahlstrom, Paragraphs [0022] and [0031], The system has two card readers, one inside and one outside the building. The card readers are in communication with the main unit. The term challenge data is interpreted as the interrogation signal as is well known in the art.**), and judges whether or not the access code received from the smart card matches the access code stored in memory (**Ahlstrom, Paragraphs [0028] and [0031]**), and**

**a card reader (**Ahlstrom, Fig. 1: 112, 114**).**

Ahlstrom does not teach:

**The certification information is a secret key,**

**the authentication information is a public key that corresponds to the secret key,**

**the authentication apparatus generates challenge data, and outputs the generated challenge data to the IC card via the card reader,**

**the IC card receives the challenge data from the authentication apparatus, generates a digital signature of the received challenge data using the secret key, and outputs the generated digital signature as response data, to the authentication apparatus via the card reader, and**

**the authentication apparatus receives the response data from the IC card, and then performs an authentication by performing a signature verification on the received digital signature using the public key and the challenge data.**

Gasser teaches:

**The certification information is a secret key (**Gasser, Col. 5, Lines 54-55, Where a private key is a secret key (see Gasser, Col. 5, Lines 20-25).**),**

**the authentication information is a public key that corresponds to the secret key (**Gasser, Col. 5, Lines 25-30, Where the public key is used to interpret the data corresponding to the private key.**),**

**the authentication apparatus generates challenge data, and outputs the generated challenge data to the IC card via the card reader (**Gasser, Col. 5, Lines 48-52, Gasser further discloses using the nonce procedure for verifying smart cards (see Gasser, Col. 12, Lines 47-51).**),**

**the IC card receives the challenge data from the authentication apparatus, generates a digital signature of the received challenge data using the secret key, and outputs the generated digital signature as response data, to the authentication apparatus (**Gasser, Col. 13, Lines 1-12**), and**

**the authentication apparatus receives the response data from the IC card, and then performs an authentication by performing a signature verification on the received digital signature using the public key and the challenge data (**Gasser, Col. 13, Lines 12-19**).**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the access control system in Ahlstrom by incorporating the teaching of private and public keys as taught by Gasser.

The motivation would be to use a well-known RSA cryptography method to authenticate a person in order to provide access control while maintaining data security.

Claim 24, Ahlstrom teaches:

**The authentication generates challenge data, and outputs the generated challenge data to the IC card via the card reader, the IC card receives the challenge data from the authentication apparatus, and the authentication apparatus receives the response data from the IC card (**Ahlstrom, Paragraphs [0022] and [0031], The system has two card readers, one inside and one outside the building. The card readers are in communication with the main unit. The term challenge data is interpreted as the interrogation signal as is well known in the art.**), and judges whether or not the access code received from the smart card matches the access code stored in memory (**Ahlstrom, Paragraphs [0028] and [0031]**), and**

**a card reader (**Ahlstrom, Fig. 1: 112, 114**).**

Ahlstrom does not teach:

**The certification information is a secret key,**

**the authentication information is a public key that corresponds to the secret key,**

**the authentication apparatus generates challenge data, generates encrypted challenge data by encrypting the generated challenge data using the public key, and outputs the generated encrypted challenge data to the IC card via the card reader,**

**the IC card receives the encrypted challenge data from the authentication apparatus, generates response data by decrypting the received encrypted challenge data using the secret key, and outputs the generated response data to the authentication apparatus via the card reader, and**

**the authentication apparatus receives the response data from the IC card, and performs an authentication by judging whether or not the received response data matches the challenge data.**

Gasser teaches:

**The certification information is a secret key (**Gasser, Col. 5, Lines 54-55, Where a private key is a secret key (see Gasser, Col. 5, Lines 20-25).**),**

**the authentication information is a public key that corresponds to the secret key (**Gasser, Col. 5, Lines 25-30, Where the public key is used to interpret the data corresponding to the private key.**),**

**the authentication apparatus generates challenge data, generates encrypted challenge data by encrypting the generated challenge data using the public key (**Gasser, Col. 5, Lines 63-68**), and outputs the generated encrypted challenge data to the IC card via the card reader (**Gasser, Col. 5, Lines 48-52,

Gasser further discloses using the nonce procedure for verifying smart cards (see Gasser, Col. 12, Lines 47-51).**),**

**the IC card receives the encrypted challenge data from the authentication apparatus, generates response data by decrypting the received encrypted challenge data using the secret key, and outputs the generated response data to the authentication apparatus via the card reader (**Gasser, Col. 13, Lines 1-12**), and**

**the authentication apparatus receives the response data from the IC card, and performs an authentication by judging whether or not the received response data matches the challenge data (**Gasser, Col. 13, Lines 12-19**).**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the access control system in Ahlstrom by incorporating the teaching of private and public keys as taught by Gasser.

The motivation would be to use a well-known RSA cryptography method to authenticate a person in order to provide access control while maintaining data security.

Claim 25, Ahlstrom in view of Gasser further teaches:

**The IC card stores therein a public key certificate that is a proof of validity for the public key, which is also contained in the public key certificate (**Gasser, Col. 5, Lines 53-68, The principal P2 represents the IC card, and the public key twoP represents the proof of validity for the public key because twoP is the public key required to decode the response data.**), and**

**the authentication apparatus further acquires the public key certificate from the IC card, performs an authentication by judging whether or not the acquired public key certificate is authentic (**Gasser, Col. 6, Lines 1-12**), and**

**if a result of the authentication is positive, stores therein the public key that is contained in the public key certificate (**Gasser, Col. 6, Lines 56-66, The system stores in the Global Naming Service a list of corresponding private and public that the system has certified.**).**

10. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ahlstrom et al. (U.S. 2003/0081747) in view of Gasser et al. (U.S. 5224163), and further in view of Yasukura (U.S. 6990588).

Claim 23, Ahlstrom in view of Gasser does not teach:

**The secret key is holder certification information that shows biometric characteristics of a holder of the IC card, and**

**the authentication apparatus further receives holder authentication information that shows biometric characteristics of a visitor, and uses the holder authentication information as the public key.**

Yasukura teaches:

**The secret key is holder certification information that shows biometric characteristics of a holder of the IC card (**Yasukura, Col. 19, Lines 9-11, The IC card

has memory installed that stores biological individuality data. The data is also encrypted (see Yasukura, Col. 17, Lines 43-47).**), and**

**the authentication apparatus further receives holder authentication information that shows biometric characteristics of a visitor, and uses the holder authentication information as the public key (**Yasukura, Col. 17, Lines 43-50, The authentication card read/write control part 411 receives the information from the IC card, and decodes the information.**).**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the smart card with encryption keys in Ahlstrom in view of Gasser, by integrating the teaching of encrypted biological individuality data as taught by Yasukura.

The motivation would be to provide additional information for identifying a person while maintaining secured information using known cryptography techniques (see Yasukura, Col. 4, Lines 35-45).

11. Claim 29 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ahlstrom et al. (U.S. 2003/0081747) in view of Abraham et al. (U.S. 4799061), and further in view of Soltesz et al. (U.S. 5756978).

Claim 29, Ahlstrom in view of Abraham does not explicitly teach:

**The converted challenge information is composed of one of an optical signal, a bar code, a QR code, an infrared signal, and an audio signal, and**

**the converted response information is composed of one of an optical signal, a bar code, a QR code, an infrared signal, and an audio signal.**

Soltesz teaches:

**Optical card readers (**Soltesz, Col. 2, Lines 53-60**).**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention that the transfer of data between the smart card and the card reader in Ahlstrom in view of Abraham is performed using one of one of an optical signal, a bar code, a QR code, an infrared signal, and an audio signal, as taught by Soltesz, and is also well-known in the art.

The motivation of using this type of signalization is to provide high speed data transmission while also being able to store more information on the cards (see Soltesz, Col. 2, Lines 65-66, and Col. 2, Lines 25-34).

12. Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ahlstrom et al. (U.S. 2003/0081747) in view of Yasukura (U.S. 6990588).

Claim 30, Ahlstrom teaches:

**The authentication apparatus further stores therein an apparatus identifier for identifying the authentication apparatus itself (**Ahlstrom, Paragraph [0028], The apparatus identifier is an access code which grants access to tenants. Because the codes are unique to the system, the access codes identify the authentication apparatus itself.**).**

Ahlstrom does not teach:

**The authentication apparatus outputs the apparatus identifier to the IC card via the card reader if the authentication apparatus judges that the visit by the forwarding agent is authentic, and**

**the IC card, upon receiving the apparatus identifier from the authentication apparatus, stores therein the received apparatus identifier.**

Yasukura teaches:

**The authentication apparatus outputs the apparatus identifier to the IC card via the card reader if the authentication apparatus judges that the visit by the forwarding agent is authentic (**Yasukura, Col. 31, Lines 25-40, When a user wishes to update the information stored on the IC card, the user must first be authenticated. Once authenticated, the user may erase old identification information.**), and**

**the IC card, upon receiving the apparatus identifier from the authentication apparatus, stores therein the received apparatus identifier (**Yasukura, Col. 31, Lines 35-40, The user enters updated information to be written on the IC card.**).**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the access control system in Ahlstrom by integrating the teaching of rewriting on an IC card as taught by Yasukura.

The motivation would be to ensure that authorized personnel will continue to have access to an access controlled system in case identification information has changed over time, such as biometric information, access code changes, etc.

13. Claim 38 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ahlstrom (U.S. 2003/0081747) in view of Gobburu et al. (U.S. 2002/0060246).

Claims 38 and 45, Ahlstrom does not teach:

**The authentication apparatus is a mobile phone.**

Gobburu teaches:

**A mobile phone with a built-in smart card reader (**Gobburu, Paragraph [0082]**).**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the access control system in Ahlstrom by incorporating the teaching of a mobile phone with a built-in smart card reader as taught by Gobburu.

The motivation would be to provide a wireless communications device capable of performing authentication, which would increase the range of the transmission of data since it is well-known in the art that mobile phones use cellular towers to transmit information over long distances. Furthermore, a mobile phone would allow the system to be placed anywhere, and not necessarily be affixed to the entrance of a residence.

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JAMES YANG whose telephone number is 571-270-5170. The examiner can normally be reached on M-F 8:30-5 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Brian Zimmerman can be reached on 571-272-3059. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/J.Y./

/Brian A Zimmerman/
Supervisory Patent Examiner, Art Unit 2612